

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2003 年 6 月 12 日 (12.06.2003)

PCT

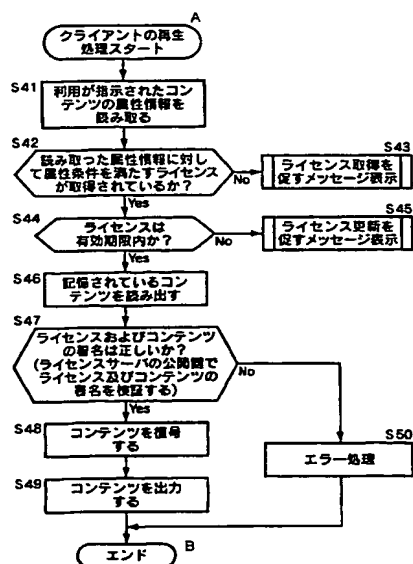
(10) 国際公開番号
WO 03/049362 A1

- (51) 国際特許分類: H04L 9/08, G06F 17/60, 15/00 (72) 発明者; および
(21) 国際出願番号: PCT/JP02/12356 (75) 発明者/出願人 (米国についてのみ): 石井 秀浩
(22) 国際出願日: 2002 年 11 月 27 日 (27.11.2002) (ISHII, Hidehiro) [JP/JP]; 〒141-0001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP).
(25) 国際出願の言語: 日本語 (74) 代理人: 稲本 義雄 (INAMOTO, Yoshio); 〒160-0023 東京都新宿区西新宿 7 丁目 1 1 番 1 8 号 7 1 1 ビルディング 4 階 Tokyo (JP).
(26) 国際公開の言語: 日本語
(30) 優先権データ: 特願2001-373674 2001 年 12 月 7 日 (07.12.2001) JP (81) 指定国 (国内): CA, CN, US.
(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川 6 丁目 7 番 3 5 号 Tokyo (JP). (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR).

[続葉有]

(54) Title: INFORMATION PROCESSING APPARATUS AND METHOD

(54) 発明の名称: 情報処理装置および方法



A...CLIENT REPRODUCTION START
S41...READ ATTRIBUTE INFORMATION OF CONTENT SPECIFIED TO BE USED
S42...LICENSE ACQUIRED SATISFIES ATTRIBUTE CONDITION FOR THE ATTRIBUTE INFORMATION READ
S43...DISPLAY MESSAGE PROMPTING TO ACQUIRE LICENSE
S44...LICENSE WITHIN A VALID TERM?
S45...DISPLAY MESSAGE PROMPTING TO UPDATE LICENSE
S46...READ OUT CONTENT STORED
S47...LICENSE AND CONTENT SIGNATURE AUTHENTIC?
(AUTHENTICATE THE LICENSE AND CONTENT SIGNATURE BY USING PUBLIC KEY OF LICENSE SERVER)
S48...DECRYPT CONTENT
S50...ERROR PROCESSING
S49...OUTPUT CONTENT
B...END

(57) Abstract: When a client reproduces a content, attribute information is read from the header of the content data corresponding to the content ID specified by the user. When the attribute information which has been read satisfies the attribute condition described in the license stored in the storage unit, encrypted content data is decrypted and output. After delivering a content, for example, by issuing a license having an attribute condition specifying a release date and artist, it is possible to sell a best version and a collection without creating a new content. If a license having a particular subscription ID as the attribute condition is defined, a user having the license can use a newly released content having the subscription ID without purchasing an additional license.

[続葉有]



添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

クライアントがコンテンツを再生する場合、ユーザが指示したコンテンツIDに対応するコンテンツデータのヘッダに記述されている属性情報を読み取る。読みとった属性情報が、記憶部に記憶されているライセンスに記述されている属性条件を満たすものである場合、暗号化されているコンテンツデータを復号して出力する。

コンテンツを配布後、例えばリリース日とアーティストを制約した属性条件を持つライセンスを発行することで、コンテンツを新たに作成することなく、ベスト版や全集を新たに発売することができる。属性条件として特定のサブスクリプションIDを持つライセンスを定義すれば、そのライセンスを持っているクライアントは、そのサブスクリプションIDを持つ新譜のコンテンツを、ライセンスを追加購入することなく使用することができる。

明細書

情報処理装置および方法

技術分野

- 5 本発明は、情報処理装置および方法に関し、特に、著作権者からライセンスを受けていないコンテンツが不正にコピーされ、利用されるのを防止することができするようにした、情報処理装置および方法に関する。

背景技術

- 10 最近、インターネットを介して、ユーザが、自分自身が保持している音楽データを他のユーザに提供し、自分自身が保持していない音楽データを他のユーザから提供を受けるようにして、複数のユーザが無料で音楽データを交換しあうシステムが実現されている。

- 15 このようなシステムでは、理論的には、1つの音楽、その他のコンテンツが存在すれば、他の全てのユーザが、それを利用することが可能となり、多くのユーザがコンテンツを購入しなくなるため、コンテンツに関する著作権者は、著作物としてのコンテンツが売れないため、著作物の販売に伴い、本来受け取ることが可能な著作物の利用に関するロイヤリティを受け取る機会を失うことになる。

- 20 そこで、配布されるコンテンツは暗号化しておき、そのコンテンツを利用するためのライセンスを別途発行し、暗号化されたコンテンツに対応するライセンスを持っていないとコンテンツを復号、再生できないようにするようにしたシステムがある。

このようにすることでコンテンツを自由に配布することを可能としつつ、著作物の著作権を保護することができる。

- 25 しかしながら、上記のシステムでは、ライセンスとコンテンツの対応関係を柔軟に設定したり、既に配布されたライセンスによって利用できるコンテンツを新たに配布することが難しかった。

発明の開示

本発明はこのような状況に鑑みてなされたものであり、コンテンツは自由に配布・流通させ、ライセンスによって利用できるコンテンツの集合を自由に設定することができるようとするものである。

本発明の第1の情報処理装置は、暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信手段と、前記コンテンツを記憶するコンテンツ記憶手段と、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信手段と、前記ライセンスを記憶するライセンス記憶手段と、前記コンテンツの前記属性情報が、前記ライセンス記憶部に記憶されているライセンスの属性条件を満たすか否かを判定する判定手段と、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号手段と、前記復号手段により復号されたコンテンツデータを出力する出力手段とを備えることを特徴とする。

前記コンテンツは、更に前記コンテンツデータを復号するためのコンテンツキーを含むようにすることができる。

前記属性情報は、属性項目と属性値の組み合わせから構成することができる。

前記属性項目はレコード会社、アーティスト、リリース日、コンテンツ発行者、ジャンル、サブスクリプション、またはレーベルに関する情報を含むようにすることができる。

前記属性条件は属性項目、属性値、及び演算子の組み合わせから構成することができる。

本発明の第2の情報処理装置は、コンテンツに含まれる属性情報に関する条件を記載した属性条件を含むライセンスを一意に識別するライセンスIDを含むライセンス要求を受信する受信手段と、ライセンスをライセンスIDと共に記憶する記憶手段と、前記ライセンス要求に含まれる前記ライセンスIDに対応する前

記ライセンスを取り込む取り込み手段と、前記ライセンスに電子署名を付加する署名手段と、署名手段により署名されたライセンスを送信する送信手段とを備えることを特徴とする。

- 5 更に、前記取り込み手段によって取り込まれたライセンスに端末 ID を付加するライセンス処理手段を備えることができる。

- 本発明の第 3 の情報処理装置は、暗号化コンテンツデータと属性情報とを含むコンテンツを記憶する記憶手段と、コンテンツを一意に識別するコンテンツ ID を含むコンテンツ要求を受信する受信手段と、コンテンツ要求に含まれるコンテンツ ID に対応するコンテンツを送信する送信手段とを備える情報処理装置であ
10 って、前記コンテンツに含まれる前記属性情報は、当該コンテンツを利用する際にライセンスの属性条件を満たすか否かを判断するために用いられる情報であり、前記ライセンスの属性条件は利用できる前記コンテンツの前記属性情報に関する条件を記載した情報であることを特徴とする。

- 本発明の情報処理方法は、暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、前記コンテンツを記憶するコンテンツ記憶ステップと、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、前記ライセンスを記憶するライセンス記憶ステップと、前記コンテンツの前記属性情報が、前記ライセンス記憶部に記憶されているライセンスの属性条件を満たすか否かを
15 判定する判定ステップと、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、前記復号手段により復号されたコンテンツデータを出力する出力ステップとを含むことを特徴とする。

- 本発明のプログラムは、暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、前記コンテンツを記憶するコンテンツ記憶ステップと、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、前記ライセン
25

5 スを記憶するライセンス記憶ステップと、前記コンテンツの前記属性情報が、前記ライセンス記憶部に記憶されているライセンスの属性条件を満たすか否かを判定する判定ステップと、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、前記復号手段により復号されたコンテンツデータを出力する出力ステップとをコンピュータに実行させるプログラムである。

10 本発明のプログラム格納媒体に格納されているプログラムは、暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、前記コンテンツを記憶するコンテンツ記憶ステップと、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、前記ライセンスを記憶するライセンス記憶ステップと、前記コンテンツの前記属性情報が、前記ライセンス記憶部に記憶されているライセンスの属性条件を満たすか否かを判定する判定ステップと、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、前記復号手段により復号されたコンテンツデータを出力する出力ステップとをコンピュータに実行させるプログラムである。

20 図面の簡単な説明

図1は、本発明を適用したコンテンツ提供システムの構成を示すブロック図である。

図2は、図1のクライアントの構成を示すブロック図である。

25 図3は、図1のクライアントのコンテンツのダウンロード処理を説明するフローチャートである。

図4は、図1のコンテンツサーバのコンテンツ提供処理を説明するフローチャートである。

図 5 は、データフォーマットの例を示す図である。

図 6 は、属性項目の種類を説明する図である。

図 7 は、ライセンスの構成を示す図である。

図 8 は、クライアントの再生処理を説明するフローチャートである。

5 図 9 は、ライセンス取得処理を説明するフローチャートである。

図 10 は、ライセンス取得処理を説明するフローチャートである。

図 11 は、ライセンス取得処理を説明するフローチャートである。

図 12 は、ライセンス取得処理の詳細を説明するフローチャートである。

図 13 は、コンテンツデータを取得する処理を説明するフローチャートである。

10 図 14 は、キーの構成を説明する図である。

図 15 は、キーの構成とライセンスの関係を説明する図である。

図 16 は、ライセンスサーバのライセンス付与処理を説明する図である。

発明を実施するための最良の形態

15 図 1 は、本発明を適用したコンテンツ提供システムの構成を示している。インターネット 2 には、クライアント 1-1, 1-2 (以下、これらのクライアントを個々に区別する必要がない場合、単にクライアント 1 と称する) が接続されている。この例においては、クライアントが 2 台のみ示されているが、インターネット 2 には、任意の台数のクライアントが接続される。

20 また、インターネット 2 には、クライアント 1 に対してコンテンツを提供するコンテンツサーバ 3、コンテンツサーバ 3 が提供するコンテンツを利用するのに必要なライセンスをクライアント 1 に対して付与するライセンスサーバ 4、およびクライアント 1 がライセンスを受け取った場合に、そのクライアント 1 に対して課金処理を行う課金サーバ 5 が接続されている。

25 これらのコンテンツサーバ 3、ライセンスサーバ 4、および課金サーバ 5 も、任意の台数、インターネット 2 に接続される。

図 2 はクライアント 1 の構成を表している。

図 2 において、CPU (Central Processing Unit) 21 は、ROM (Read Only Memory) 22 に記憶されているプログラム、または記憶部 28 から RAM

(Random Access Memory) 23 にロードされたプログラムに従って各種の処理
5 RAM 23 にはまた、CPU 21 が各種の処理を実行する上において必要なデータな
ども適宜記憶される。

暗号化復号部 24 は、コンテンツデータを暗号化するとともに、既に暗号化さ
れているコンテンツデータを復号する処理を行う。コーデック部 25 は、例えば、
ATRAC (Adaptive Transform Acoustic Coding) 3 方式などでコンテンツデー
10 タをエンコードし、入出力インタフェース 32 を介してドライブ 30 に接続され
ている半導体メモリ 44 に供給し、記録させる。あるいはまた、コーデック部 2
5 は、ドライブ 30 を介して半導体メモリ 44 より読み出した、エンコードされ
ているデータをデコードする。

半導体メモリ 44 は、例えば、メモリスティック (商標) などにより構成され
15 る。

CPU 21、ROM 22、RAM 23、暗号化復号部 24、およびコーデック部 25 は、
バス 31 を介して相互に接続されている。このバス 31 にはまた、入出力インタ
フェース 32 も接続されている。

入出力インタフェース 32 には、キーボード、マウスなどよりなる入力部 26、
20 CRT、LCD などよりなるディスプレイ、並びにスピーカなどよりなる出力部 27、
ハードディスクなどより構成される記憶部 28、モデム、ターミナルアダプタな
どより構成される通信部 29 が接続されている。通信部 29 は、インターネット
2 を介しての通信処理を行う。通信部 29 はまた、他のクライアントとの間で、
アナログ信号またはデジタル信号の通信処理を行う。

25 入出力インタフェース 32 にはまた、必要に応じてドライブ 30 が接続され、
磁気ディスク 41、光ディスク 42、光磁気ディスク 43、或いは半導体メモリ

4 4 などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部 2 8 にインストールされる。

5 なお、図示は省略するが、コンテンツサーバ 3、ライセンスサーバ 4、課金サーバ 5 も、図 2 に示したクライアント 1 と基本的に同様の構成を有するコンピュータにより構成される。

次に、図 3 のフローチャートを参照して、クライアント 1 がコンテンツサーバ 3 からコンテンツの提供を受ける処理について説明する。

ユーザが、入力部 2 6 を操作することでコンテンツサーバ 3 に対するアクセスを指令すると、CPU 2 1 は、通信部 2 9 を制御し、インターネット 2 を介してコンテンツサーバ 3 にアクセスさせる。ステップ S 2 において、ユーザが、入力部 2 6 を操作して、提供を受けるコンテンツを指定すると、CPU 2 1 は、この指定情報を受け取り、通信部 2 9 から、インターネット 2 を介してコンテンツサーバ 3 に、指定されたコンテンツのコンテンツ ID を通知する。図 4 のフローチャートを参照して後述するように、この通知を受けたコンテンツサーバ 3 は、通知されたコンテンツ ID に対応する、暗号化されたコンテンツデータを含むコンテンツを送信してくるので、ステップ S 3 において、CPU 2 1 は、通信部 2 9 を介して、このコンテンツを受信すると、ステップ S 4 において、コンテンツを記憶部 2 8 を構成するハードディスクに供給し、記憶させる。

次に、図 4 のフローチャートを参照して、クライアント 1 の以上の処理に対応するコンテンツサーバ 3 のコンテンツ提供処理について説明する。なお、以下の説明において、図 2 のクライアント 1 の構成は、コンテンツサーバ 3 の構成としても引用する。

ステップ S 2 1 において、コンテンツサーバ 3 の CPU 2 1 は、インターネット 2 から通信部 2 9 を介してクライアント 1 よりアクセスを受けるまで待機し、アクセスを受けたと判定したとき、ステップ S 2 2 に進み、クライアント 1 から送信されてきたコンテンツを指定するコンテンツ ID を取り込む。このコンテンツ

を指定する情報は、クライアント1が、図3のステップS2において通知してきたコンテンツIDである。

ステップS23において、コンテンツサーバ3のCPU21は、記憶部28に記憶されているコンテンツデータの中から、ステップS22の処理で取り込まれた
5 情報で指定されたコンテンツを読み出す。CPU21は、ステップS24において、記憶部28から読み出されたコンテンツデータを、暗号化復号部24に供給し、暗号化させる。

記憶部28に記憶されているコンテンツデータは、コーデック部25により、既にATRAC3方式によりエンコードされているので、このエンコードされている
10 コンテンツデータが暗号化されることになる。

なお、もちろん、記憶部28に予め暗号化した状態でコンテンツデータを記憶させることができる。この場合には、ステップS24の処理は省略することが可能である。

次に、ステップS25において、コンテンツサーバ3のCPU21は、暗号化したコンテンツデータを伝送するフォーマットを構成するヘッダに、暗号化されて
15 いるコンテンツデータを復号するのに必要なキーと、コンテンツに関する各種情報を示す属性情報を付加する。そして、ステップS26において、コンテンツサーバ3のCPU21は、ステップS24の処理で暗号化されたコンテンツデータと、ステップS25の処理でキーと属性情報及びその電子署名を付加したヘッダとを
20 フォーマット化したコンテンツを、通信部29から、インターネット2を介して、アクセスしてきたクライアント1に送信する。

図5は、このようにして、コンテンツサーバ3からクライアント1にコンテンツが供給される場合のフォーマットの構成を表している。同図に示されるように、このフォーマットは、ヘッダ(Header)とデータ(Data)とにより構成される。

25 ヘッダには、属性情報(Attribute List)及び属性情報をライセンスサーバの暗号鍵で署名した電子署名、イネーブリングキーブロック(EKB(Enabling Key Block))および、EKBをDNKを用いて復号処理することによって得られる

ルートキーKRにより暗号化されたコンテンツキーKc (KR (Kc)) が配置されている。

属性情報には属性項目と属性値との組み合わせからなる属性のエントリーが複数記述されている。

- 5 属性項目の種類を図6に示す。CID、RCID、CIID、AID、GID及びLIDはそれぞれコンテンツ、レコード会社、コンテンツ発行者、アーティスト、ジャンル及びレーベルを一意に識別するIDである。RelDateはコンテンツのリリース日を表す。サブスクリプションIDは後述するサブスクリプションライセンスに用いられる属性項目である。

- 10 URLは、コンテンツを利用するためのライセンスを取得するときアクセスするアドレス情報であり、図1のシステムの場合、具体的には、ライセンスを受けるために必要なライセンスサーバ4のアドレスである。

- データは、任意の数の暗号化ブロック (Encryption block) により構成される。各暗号化ブロックは、イニシャルベクトル (IV (Initial Vector))、シード (Seed)、およびコンテンツデータをキーK'cで暗号化したデータ EK'
15 c(data)により構成されている。

キーK'cは、次式により示されるように、コンテンツキーKcと、乱数で設定される値Seedをハッシュ関数に適応して演算された値により構成される。

$$K'c = \text{Hash}(Kc, \text{Seed})$$

- 20 イニシャルベクトルIVとシードSeedは、各暗号化ブロック毎に異なる値に設定される。

この暗号化は、コンテンツのデータを8バイト単位で区分して、8バイト毎に行われる。後段の8バイトの暗号化は、前段の8バイトの暗号化の結果を利用して行われるCBC (Cypher Block Chaning) モードで行われる。

- 25 CBCモードの場合、最初の8バイトのコンテンツデータを暗号化するとき、その前段の8バイトの暗号化結果が存在しないため、最初の8バイトのコンテンツ

データを暗号化するときは、イニシャルベクトル IV を初期値として暗号化が行われる。

この CBC モードによる暗号化を行うことで、1つの暗号化ブロックが解読されたとしても、その影響が、他の暗号化ブロックにおよぶことが抑制される。

- 5 なお、この暗号化については、図 14 と図 15 を参照にして、後に詳述する。

以上のようにして、クライアント 1 は、コンテンツサーバ 3 からコンテンツを無料で、自由に取得することができる。

しかしながら、各クライアント 1 は、取得したコンテンツを利用するとき、ライセンスを取得する必要がある。

- 10 ライセンスを取得する際には、クライアント 1 は事前にライセンスサーバにオンラインあるいはオフラインで登録処理を行い、サービスデータを取得しておく。サービスデータにはデバイスノードキー (DNK) 及び端末 ID が含まれており、EKB を復号処理するのに用いられる。サービスデータ及びライセンスサーバから取得するライセンスはクライアント 1 の記憶部 28 にセキュアに保存される。

- 15 図 7 にライセンスの構成を示す。ライセンスにはライセンス ID、タイムスタンプ、使用期限、属性条件、使用規則、及びこれらをライセンスサーバの秘密鍵で署名した電子署名が含まれる。タイムスタンプはライセンスの発行日を表す。使用期限はライセンスを使用できる期限日を表し、この期限日を過ぎるとそのライセンスは使用できなくなる。属性条件はそのライセンスを所持しているクライアント 1 が利用できるコンテンツの属性の条件を属性項目と属性項目に関する値、
20 比較演算子、及び論理演算子の組み合わせからなる条件式によって表したものである。使用規則にはそのライセンスの利用できるコンテンツを使用するための規則を記述したものであり、サービスデータに含まれているものと同じ端末 ID が含まれる。

- 25 以下に、コンテンツに含まれる属性情報、及びライセンスに含まれる属性条件との組み合わせによって実現可能なライセンス構成の例を示す。

コンテンツ c1 の属性情報には、次のように記述されている。

c1: cid = {1}, aid = {0, 1}, reldate = 2000 年 11 月 10 日

これは、コンテンツ ID は 1、アーティスト ID は 0 および 1（即ち、0 番のアーティストと 1 番のアーティストの合作）、リリース日は 2000 年 11 月 10 日であるということを表す。

- 5 同様に、コンテンツ c2, c3, c4 の属性情報に、次のように記述されている。

c2: cid = {2}, aid = {0}, reldate = 2000 年 12 月 20 日

c3: cid = {3}, aid = {0}, reldate = 2001 年 3 月 1 日

c4: cid = {4}, aid = {0}, reldate = 2001 年 10 月 21 日

一方、ライセンス 11 の属性条件には、次のように記述されている。

- 10 11: cid \supseteq 1 \vee cid \supseteq 2

これにより、利用権 r1 はコンテンツ c1 と c2 に対応する。即ち、利用権 r1 を保有している端末では、コンテンツ c1 と c2 を利用する事ができる。

ライセンス 12 の属性条件は、次のように記述されている。

12: aid \supseteq 0 \wedge (2001 年 1 月 1 日 < reldate < 2001 年 12 月 31 日)

- 15 これは、2001 年にリリースされた 0 番のアーティストのコンテンツ、という意味の条件であり、ライセンス 12 はコンテンツ c3 と c4 に対応する。この時点で、ライセンス 12 を保有している端末では、コンテンツ c3 と c4 を利用する事ができる。後に下記のような属性情報を持たせたコンテンツ c5 が発行されたとする。

- 20 c5: cid = {5}, aid = {0}, reldate = {2001 年 12 月 1 日}

このコンテンツをコンテンツサーバ 3 からダウンロードするなどして入手すると、既にライセンス 12 を保有しているクライアント 1 では、新たにライセンスサーバ等に接続する必要なく、コンテンツ c5 も利用できるようになる。

これらのコンテンツの配布後、配信事業者が新たにベスト版としてコンテンツ

- 25 c1, c2, c5 を組み合わせて発売しようとするならば、それに対応する次のようなライセンス 13 を発行すれば、コンテンツを新たに作成する必要なく、配布済み・流通中のコンテンツをそのまま活用して、ベスト版発売が可能である。

13: $\text{cid} \ni 1 \vee \text{cid} \ni 2 \vee \text{cid} \ni 5$

このようにして、配布済み・流通中のコンテンツを組み合わせた利用権を容易に新規発行できる。例えば、リリース日とアーティストを制約した属性条件を持つライセンスを発行することで、あるアーティストの特定の年代にリリースされた作品を含む全集を新たに発売することができる。

また、アーティストを制約した属性条件を持つライセンスを発行することで、あるグループの全集（グループによる作品、グループのメンバーのソロ作品などを含む）を新たに発売することができる。

次に、サブスクリプション・サービスとして、毎月いくつかの新譜を追加利用できるようにするライセンスを定義する例を示す。

ライセンス 14 の属性の条件を、次のように定義する。

14: $\text{cid} \ni 3 \vee \text{cid} \ni 4 \vee \text{sid} \ni 1$

このライセンス 14 を所持しているクライアント 1 では、まず、既に発行されているコンテンツ c3 と c4 が利用可能である。翌月、新譜として次のような属性情報を持ったコンテンツ c6 と c7 が発行されたとする。

c6: $\text{cid} = \{6\}$, $\text{sid} = \{1\}$

c7: $\text{cid} = \{7\}$, $\text{sid} = \{1\}$

この場合、ライセンス 14 を持っているクライアント 1 は、新たにライセンスを購入する必要なく、コンテンツ c6 と c7 を利用する事ができる。同様にして、月ごとにサブスクリプション ID に 1 を含んだコンテンツを発行する事により、ライセンス 14 を持っているクライアント 1 はライセンスを別途購入することなく、利用可能なコンテンツを追加していく事ができる。

このように、属性条件を属性項目、属性値、及び論理演算子、関係演算子等の演算子の組み合わせで表すことで、利用できるコンテンツの集合を柔軟に設定できるようにする。

属性条件に含まれる演算子はここに挙げられているに限定されず、その他の各種演算子を利用することができる。

図 8 を参照して、クライアント 1 がコンテンツを再生する場合の処理について説明する。

ステップ S 4 1 において、クライアント 1 の CPU 2 1 は、ユーザが入力部 2 6 を操作することで指示したコンテンツ ID を取得する。

- 5 そして、CPU 2 1 は、コンテンツ ID を取得すると該当するコンテンツデータのヘッダに記述されている属性情報を読み取る。

次に、ステップ S 4 2 に進み、CPU 2 1 は、ステップ S 4 1 で読み取られた属性情報が各ライセンスに記述されている属性条件を満たすライセンスが、クライアント 1 により既に取得され、記憶部 2 8 に記憶されているか否かを判定する。

- 10 そのようなライセンスが見つからなかった場合には、ステップ S 4 3 に進み、CPU 2 1 は、出力部 2 7 を介して、ディスプレイにライセンスの取得を促すメッセージを表示する。

- ステップ S 4 2 において、ライセンスが既に取得されていると判定された場合、ステップ S 4 4 に進み、CPU 2 1 は、取得されているライセンスは有効期限内のものであるか否かを判定する。ライセンスが有効期限内のものであるか否かは、
15 ライセンスの内容として規定されている期限と、タイマ 2 0 により計時されている現在日時と比較することがで判断される。ライセンスの有効期限が既に満了していると判定された場合、CPU 2 1 は、ステップ S 4 5 に進み、ライセンス更新処理を実行する。このライセンス更新処理の詳細は、図 8 のフローチャートを参
20 照して後述する。

- ステップ S 4 4 において、ライセンスはまだ有効期限内であると判定された場合、または、ステップ S 4 5 において、ライセンスが更新された場合、ステップ S 4 5 に進み、CPU 2 1 は、コンテンツのヘッダに含まれる電子署名及びライセンスに含まれる電子署名をライセンスサーバ 4 の公開鍵で検証する。電子署名の
25 検証の結果、電子署名が正しいと判断された場合、ステップ S 4 6 に進み、CPU 2 1 は、暗号化されているコンテンツデータを記憶部 2 8 から読み出し、RAM 2 3 に格納させる。そして、ステップ S 4 7 において、CPU 2 1 は、RAM 2 3 に記

憶された暗号化ブロックのデータを、図 5 のデータに配置されている暗号化ブロック単位で、暗号化復号部 2 4 に供給し、復号させる。

CPU 2 1 は、さらに、ステップ S 4 8 において、暗号化復号部 2 4 により復号されたコンテンツデータをコーデック部 2 5 に供給し、デコードさせる。そして、
5 コーデック部 2 5 によりデコードされたデータを、CPU 2 1 は、入出力インタフェース 3 2 から出力部 2 7 に供給し、D/A 変換させ、スピーカから出力させる。

図 9 乃至図 11 を用いてクライアントがライセンスサーバ 4 からライセンスを取得する処理を説明する。

図 9 はクライアント 1 のユーザが利用したいコンテンツが決まっている場合の
10 ライセンス取得処理を示している。ユーザが、入力部 2 6 を操作することでコンテンツを指定しライセンスサーバ 4 にライセンスリストの要求を指示すると、CPU 2 1 は、通信部 2 9 を制御し、インターネット 2 を介してコンテンツサーバ 3 に指定されたコンテンツのコンテンツ ID を含むライセンスリスト要求を送信する。ライセンスサーバ 4 はライセンスリスト要求を受信すると、受信したライ
15 センスリストに含まれるコンテンツ ID から、該当するコンテンツを利用可能なライセンスを抽出し、各ライセンスのライセンス ID、ライセンス名、利用できるコンテンツの条件、現在利用できるコンテンツのリスト、コンテンツの使用条件等を記載したライセンスリストをクライアント 1 に送信する。

クライアント 1 がライセンスサーバ 4 からライセンスリストを受信すると、
20 CPU 2 1 は、出力部 2 7 にライセンスリストに含まれる各ライセンスの情報を表示する。ユーザがその情報を参照し、所望するライセンスを選択すると、CPU 2 1 は、通信部 2 9 を制御し、SSL などの相互認証によりセッションを形成した後、インターネット 2 を介してコンテンツサーバ 3 に、選択されたライセンスのライセンス ID と端末 ID と課金用のユーザ ID 及びパスワードを含むライセンス要求
25 を暗号化して送信する。ライセンスサーバ 4 はクライアント 1 から送信されたライセンス要求を受信すると、後述するライセンス発行処理を行った後、ライセンス要求に含まれるライセンス ID に対応するライセンスをクライアント 1 に送信

する。クライアント 1 はライセンスサーバ 4 から送信されたライセンスを受信すると、受信したライセンスを暗号化等をしてセキュアな状態で記憶部 28 に保存する。

- 5 以上のようにして、ユーザはクライアント 1 が既に所持しているコンテンツを利用するためのライセンスを取得することができる。以上のライセンス取得処理は、ユーザがクライアントに所持しているコンテンツを再生する操作した際に、そのコンテンツを再生するためのライセンスを取得していなかった場合、自動的に開始されるようにしても良い。

- 次に、ユーザが各種検索条件を指定してライセンスを検索し、取得する処理を
10 図 16 に示す。まず、ユーザが欲しいライセンスを検索するための、ライセンス名、ライセンスの種類、ライセンスが利用可能とするコンテンツのタイトル、アルバム名、ジャンル、アーティスト名、リリース日等の検索条件を入力部 26 を操作することによって指定すると、CPU 21 は、通信部を制御し、入力された検索条件をフォーマットしたデータを含むライセンスリスト要求をコンテンツサーバ 3 に送信する。コンテンツサーバはクライアント 1 から送信されたライセンス
15 リスト要求を受信すると、ライセンスリスト要求に含まれる検索条件を満たすライセンスを記憶部 28 から検索し、ライセンス ID 等の各ライセンスに関する情報を含むライセンスリストをクライアント 1 に送信する。

- クライアント 1 がライセンスサーバ 4 からライセンスリストを受信すると、
20 CPU 21 は、出力部 27 にライセンスリストに含まれる各ライセンスの情報を表示する。ユーザがその情報を参照し、所望するライセンスを選択すると、CPU 21 は、通信部 29 を制御し、SSL などの相互認証によりセッションを形成した後、インターネット 2 を介してコンテンツサーバ 3 に、選択されたライセンスのライセンス ID と端末 ID と課金用のユーザ ID 及びパスワードを含むライセンス要求
25 を暗号化して送信する。ライセンスサーバ 4 はクライアント 1 から送信されたライセンス要求を受信すると、後述するライセンス発行処理を行った後、ライセンス要求に含まれるライセンス ID に対応するライセンスをクライアント 1 に送信

する。クライアント 1 はライセンスサーバ 4 から送信されたライセンスを受信すると、受信したライセンスを暗号化するなどしてセキュアな状態で記憶部 28 に保存する。

5 以上のようにして、ユーザは欲しいライセンスを検索し、取得することができる。

次に、ユーザが欲しいライセンスのライセンス ID を知っている場合のライセンス取得処理を図 11 に示す。

ユーザがライセンス ID を入力部 26 を操作し入力して、欲しいライセンスの
10 ライセンス ID を指定すると、CPU 21 は、通信部 29 を制御し、SSL などの相互
認証によりセッションを形成した後、インターネット 2 を介してコンテンツサーバ 3 に、選択されたライセンスのライセンス ID と端末 ID と課金用のユーザ ID
及びパスワードを含むライセンス要求を暗号化して送信する。ライセンスサーバ
4 はクライアント 1 から送信されたライセンス要求を受信すると、後述するライ
15 センス発行処理を行った後、ライセンス要求に含まれるライセンス ID に対応す
るライセンスをクライアント 1 に送信する。クライアント 1 はライセンスサーバ
4 から送信されたライセンスを受信すると、受信したライセンスを暗号化等をし
てセキュアな状態で記憶部 28 に保存する。

20 以上のようにして、ユーザは雑誌などに記載されているライセンスの広告など
からライセンス ID を知り、そのライセンス ID を指定することで所望するライ
センスを取得することができる。

また、Web サイトの HTML ファイルや電子メール等にライセンス ID を含むラ
イセンスサーバの URL のリンク情報が記載されており、これをユーザがクリッ
クするなどして選択することでライセンス取得処理を開始するようにしても良い。

25 図 12 のフローチャートを参照して、図 9 乃至図 11 におけるライセンス発行
処理の詳細を説明する。なお、この場合においても、図 2 のクライアント 1 の構
成は、ライセンスサーバ 4 の構成としても引用される。

最初にステップS 1 0 2において、CPU 2 1はライセンス要求に含まれるライセンス ID、端末 ID、ユーザ ID、パスワードを取り込む。

そして、ライセンスサーバ4のCPU 2 1は、通信部 2 9から課金サーバ5にアクセスし、ユーザ ID とパスワードに対応するユーザの与信処理を要求する。課金サーバ5は、インターネット 2を介してライセンスサーバ4から与信処理の要求を受けると、そのユーザ ID とパスワードに対応するユーザの過去の支払い履歴などを調査し、そのユーザが、過去にライセンスの対価の不払いの実績があるか否かなどを調べ、そのような実績がない場合には、ライセンスの付与を許容する与信結果を送信し、不払いの実績などがある場合には、ライセンス付与の不許可の与信結果を送信する。

ステップS 1 0 4において、ライセンスサーバ4のCPU 2 1は、課金サーバ5からの与信結果が、ライセンスを付与することを許容する与信結果であるか否かを判定し、ライセンスの付与が許容されている場合には、ステップS 1 0 5に進み、ライセンス ID に対応するライセンスをデータベースから取り出し、ライセンスの使用規則のフィールドに端末 ID を挿入し、ライセンスサーバ4の秘密鍵で電子署名を生成、付加する。

そして、ステップS 1 0 7に進み、ライセンスサーバ4のCPU 2 1は、その端末 ID と電子署名が付加されたライセンスを通信部 2 9からインターネット 2を介してクライアント 1に送信させる。

ステップS 1 0 8においてライセンスサーバ4のCPU 2 1は、ステップS 1 0 7の処理で、いま送信したライセンスをステップS 1 0 2の処理で取り込まれたユーザ ID とパスワードに対応して、記憶部 2 8に記憶させる。さらに、ステップS 1 0 9において、CPU 2 1は、課金処理を実行する。具体的には、CPU 2 1は、通信部 2 9から課金サーバ5に、そのユーザ ID とパスワードに対応するユーザに対する課金処理を要求する。課金サーバ5は、この課金の要求に基づいて、そのユーザに対する課金処理を実行する。上述したように、この課金処理に対して、そのユーザが支払いを行わなかったような場合には、以後、そのユーザは、

ライセンスの付与を要求したとしても、ライセンスを受けることができないことになる。

すなわち、この場合には、課金サーバ5からライセンスの付与を不許可とする
与信結果が送信されてくるので、ステップS104からステップS110に進み、

- 5 CPU21は、エラー処理を実行する。具体的には、ライセンスサーバ4のCPU21は、通信部29を制御してアクセスしてきたクライアント1に対して、ライセンスを付与することができない旨のメッセージを出力し、処理を終了させる。

この場合、上述したように、そのクライアント1はライセンスを受けることができないので、そのコンテンツを利用することができないことになる。

- 10 次に、図13を用いてライセンスが利用可能なコンテンツのコンテンツデータを取得する処理を説明する。

- ユーザが入力部26を操作し、ライセンスを選択すると、CPUは、通信部29を制御し、インターネット2を介してコンテンツサーバ3に、選択されたライセンスのライセンスIDを含むコンテンツリスト要求を送信する。ライセンスサーバ4はコンテンツリスト要求を受信すると、コンテンツリスト要求に含まれるライセンスIDを取り出す。ライセンスサーバ4はライセンスIDをキーとしてライセンスデータベースから、該当するライセンスによって利用可能なコンテンツを抽出する。その後、ライセンスサーバは、抽出された各コンテンツのコンテンツID、コンテンツをダウンロードするためのURL、及びコンテンツ名、アーティスト名、ジャンル等のコンテンツ情報を含む、コンテンツリストをクライアント1に送信する。
- 15
- 20

- クライアント1は出力部を制御してコンテンツリストを受信するとコンテンツリストに含まれる各コンテンツのコンテンツ情報を表示させる。ユーザが表示されたコンテンツ情報を参照して、ダウンロードするコンテンツを選択すると、クライアント1はコンテンツのURLに従って、コンテンツサーバにコンテンツ要求をコンテンツサーバ3に送信する。コンテンツサーバはコンテンツ要求を受信すると、コンテンツ要求に含まれるコンテンツIDを持つコンテンツをクライア
- 25

ント1に送信する。クライアント1はコンテンツサーバ3からコンテンツを受信すると、受信したコンテンツを記憶部28に記憶させる。

5 以上のようにして、ユーザはライセンスにより利用可能となるコンテンツを探し出し、コンテンツサーバ3からクライアントのダウンロードさせることができる。

図14は、ブロードキャストインクリプション (Broadcast Encryption) を、キーの管理方式に採用した場合におけるキーの構成方法を表している。図14に示されるように、キーは、階層ツリー構造とされ、最下段のリーフ (leaf) が個々のデバイスに対応する。図14の例の場合、番号0から番号15までの16
10 個のデバイスに対応するキーが生成される。

各キーは、図中丸印で示される各ノードに対応して規定される。この例では、最上段のルートノードに対応してキーKRが、2番目のノードに対応してキーK0、K1が、3段目のノードに対応してキーK00乃至K11が、第4番目のノードに対応してキーK000乃至キーK111が、それぞれ対応されている。そして、最下段のノードとしてのリーフ (デバイスノード) に、キーK0000乃至K1111が、それぞれ対応されている。
15

階層構造とされているため、例えば、キーK0010とキー0011の上位のキーは、K001とされ、キーK000とキーK001の上位のキーは、K00とされている。以下同様に、キーK00とキーK01の上位のキーは、K0とされ、キーK0とキーK1の上位のキーは、KRとされている。
20

コンテンツを利用するために用いるキーは、最下段のデバイスノード (リーフ) から、最上段のルートノードまでの1つのパスの各ノードに対応するキーで構成される。例えば、番号3のコンテンツを利用するキーは、キーK0011、K001、K00、K0、KRを含むリーフからルートまでのパス上の各キーで
25 構成される。

本発明のシステムにおいては、例えば、図15に示されるように、 $8 \times 24 \times 3$ 2段のノードに対応するキーで構成される階層ツリー構造キーシステムが利用

される。このキーシステムでは、ルートノードから下位の 8 段までの各ノードに対応するキーに、カテゴリが対応される。ここにおけるカテゴリとは、例えばメモリスティックなどの半導体メモリを使用する機器のカテゴリ、デジタル放送を受信する機器のカテゴリといったカテゴリを意味する。

- 5 図 15 の例では、ルートノードから 8 段目のノードのうちの 1 つのノードに、本発明のシステムが対応される。このノードよりさらに下の階層の 24 段のノードに対応するキーにより、ライセンスが対応される。これにより、約 16 メガ ($= 2^{24} = \text{約 } 160 \text{ 万}$) のライセンスを規定することができる。さらに、最も下側の 32 段の階層により、約 4 ギガ ($= 2^{32} = \text{約 } 40 \text{ 億}$) のユーザを規定することが
- 10 ことができる。最下段の 32 段のノードに対応するキーが、DNK (Device Node Key) を構成する。

- 各コンテンツは、64 ($= 8 + 24 + 32$) 段の各ノードで構成されるパスの内の 1 つに対応される。すなわち、各コンテンツの暗号化には、割り当てられたパスを構成するノードに対応するキーが用いられる。上位の階層のキーは、その
- 15 直近の下位の階層のキーを用いて暗号化され、図 5 の EKB 内に配置される。最下段の DNK は、EKB 内には配置されず、クライアントがライセンスサーバに登録するときに取得するサービスデータに記述され、図 16 に示されるように、ユーザのクライアント 1 に与えられる。

- クライアント 1 は、サービスデータに記述されている DNK を用いて、コンテンツデータとともに配布される EKB 内に記述されている直近の上位の階層のキーを復号し、復号して得たキーを用いて、EKB 内に記述されているさらにその上の階層のキーを復号する。以上の処理を順次行うことで、クライアント 1 は、そのコンテンツのパスに属するすべてのキーを得ることができる。
- 20

- クライアント 1 は以上の EKB の復号処理を行った後得られる KR を用いて、KR
- 25 によって暗号化されているコンテンツキー KR (KC) を復号し、コンテンツキー KC を得ることができる。

なお、本発明におけるキーは、図 14 および図 15 に示されるようなブロードキャストインクリプションを利用したキーシステム以外のキーで構成することも可能である。

また、本発明が適用されるクライアントは、いわゆるパーソナルコンピュータ
5 以外に、PDA (Personal Digital Assistants)、携帯電話機、ゲーム端末機など
とすることができる。

一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

この記録媒体は、図 2 に示すように、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク 4 1 (フロッピディスクを含む)、光ディスク 4 2 (CD-ROM (Compact Disk-Read
15 Only Memory), DVD (Digital Versatile Disk) を含む)、光磁気ディスク 4 3 (MD (Mini-Disk) を含む)、もしくは半導体メモリ 4 4 などよりなるパッケージメディアにより構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されている ROM 2 2 や、記憶部 2 8 に含まれるハードディスクなどで構成される。

20 なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。
25

産業上の利用可能性

- 以上の如く、本発明の情報処理装置および方法、プログラム格納媒体、並びにプログラムによれば、暗号化されたデータとコンテンツの属性情報を、所定のフォーマットにフォーマット化して、出力するようにし、ライセンスに属性条件を
- 5 ふ含むようにし、コンテンツの属性情報がライセンスの属性条件を満たす場合に暗号化されたデータを復号できるようにしたので、データが不正に利用されるのを抑制しつつ、ライセンスを柔軟に発行することが可能となる。

請求の範囲

1. 暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信手段と、
前記コンテンツを記憶するコンテンツ記憶手段と、
- 5 利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信手段と、
前記ライセンスを記憶するライセンス記憶手段と、
前記コンテンツの前記属性情報が、前記ライセンス記憶部に記憶されているライセンスの属性条件を満たすか否かを判定する判定手段と、
- 10 前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号手段と、
前記復号手段により復号されたコンテンツデータを出力する出力手段とを備えることを特徴とする情報処理装置。
- 15 2. 前記コンテンツは、更に前記コンテンツデータを復号するためのコンテンツキーを含む
ことを特徴とする請求の範囲第1項に記載の情報処理装置。
3. 前記属性情報は、属性項目と属性値の組み合わせからなる
ことを特徴とする請求の範囲第1項に記載の情報処理装置。
- 20 4. 前記属性項目はレコード会社、アーティスト、リリース日、コンテンツ発行者、ジャンル、サブスクリプション、またはレーベルに関する情報を含む
ことを特徴とする請求の範囲第1項に記載の情報処理装置。
5. 前記属性条件は属性項目、属性値、及び演算子の組み合わせからなる
ことを特徴とする請求の範囲第1項に記載の情報処理装置。
- 25 6. コンテンツに含まれる属性情報に関する条件を記載した属性条件を含むライセンスを一意に識別するライセンスIDを含むライセンス要求を受信する受信手段と、

ライセンスをライセンス ID と共に記憶する記憶手段と、
前記ライセンス要求に含まれる前記ライセンス ID に対応する前記ライセンス
を取り込む取り込み手段と、

前記ライセンスに電子署名を付加する署名手段と、

- 5 署名手段により署名されたライセンスを送信する送信手段と
を備えることを特徴とする情報処理装置。

7. 更に、前記取り込み手段によって取り込まれたライセンスに端末 ID を付
加するライセンス処理手段

を備えることを特徴とする請求の範囲第 6 項に記載の情報処理装置。

- 10 8. 暗号化コンテンツデータと属性情報とを含むコンテンツを記憶する記憶手
段と、

コンテンツを一意に識別するコンテンツ ID を含むコンテンツ要求を受信する
受信手段と、

- 15 コンテンツ要求に含まれるコンテンツ ID に対応するコンテンツを送信する送
信手段と

を備える情報処理装置であって、

前記コンテンツに含まれる前記属性情報は、当該コンテンツを利用する際にラ
イセンスの属性条件を満たすか否かを判断するために用いられる情報であり、

- 20 前記ライセンスの属性条件は利用できる前記コンテンツの前記属性情報に関す
る条件を記載した情報である

ことを特徴とする情報処理装置。

9. 暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテ
ンツ受信ステップと、

前記コンテンツを記憶するコンテンツ記憶ステップと、

- 25 利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むラ
イセンスを受信するライセンス受信ステップと、

前記ライセンスを記憶するライセンス記憶ステップと、

前記コンテンツの前記属性情報が、前記ライセンス記憶部に記憶されているライセンスの属性条件を満たすか否かを判定する判定ステップと、

前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデー

5 タを復号する復号ステップと、

前記復号手段により復号されたコンテンツデータを出力する出力ステップとを含むことを特徴とする情報処理方法。

10 暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、

10 前記コンテンツを記憶するコンテンツ記憶ステップと、

利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、

前記ライセンスを記憶するライセンス記憶ステップと、

15 前記コンテンツの前記属性情報が、前記ライセンス記憶部に記憶されているライセンスの属性条件を満たすか否かを判定する判定ステップと、

前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、

20 前記復号手段により復号されたコンテンツデータを出力する出力ステップとをコンピュータに実行させるプログラム。

11 暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、

前記コンテンツを記憶するコンテンツ記憶ステップと、

25 利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、

前記ライセンスを記憶するライセンス記憶ステップと、

前記コンテンツの前記属性情報が、前記ライセンス記憶部に記憶されているラ

イセンスの属性条件を満たすか否かを判定する判定ステップと、

前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、

- 5 前記復号手段により復号されたコンテンツデータを出力する出力ステップとをコンピュータに実行させるプログラムが格納されたプログラム格納媒体。

1/14

図1

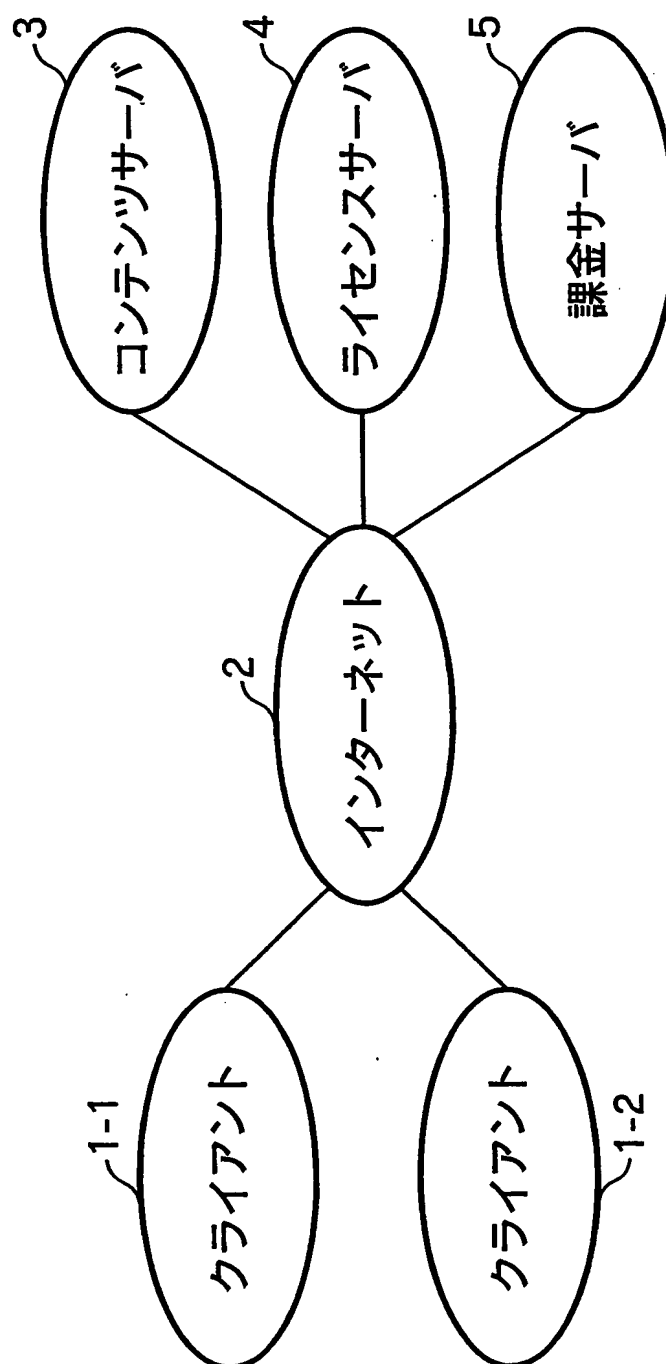
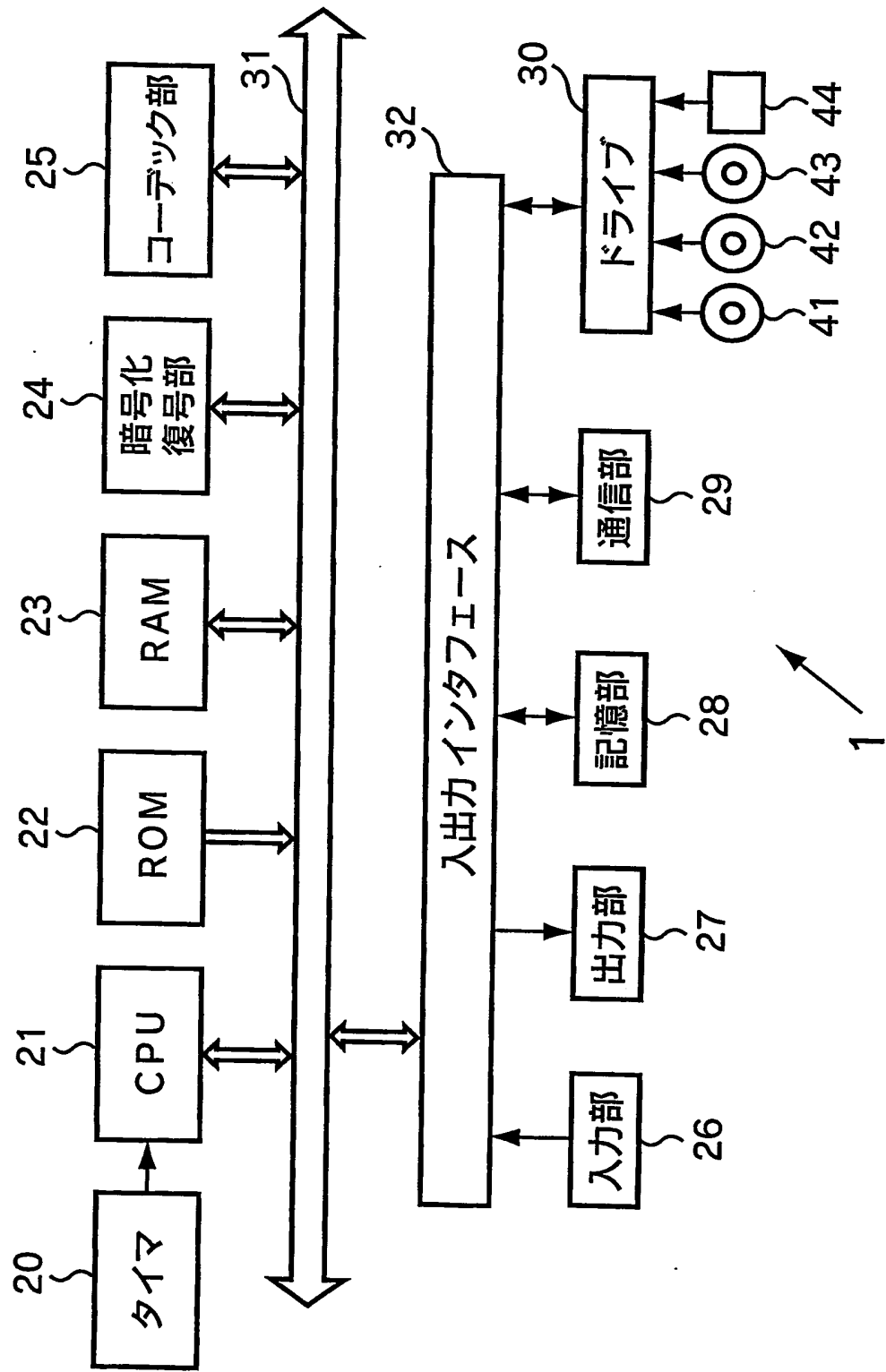
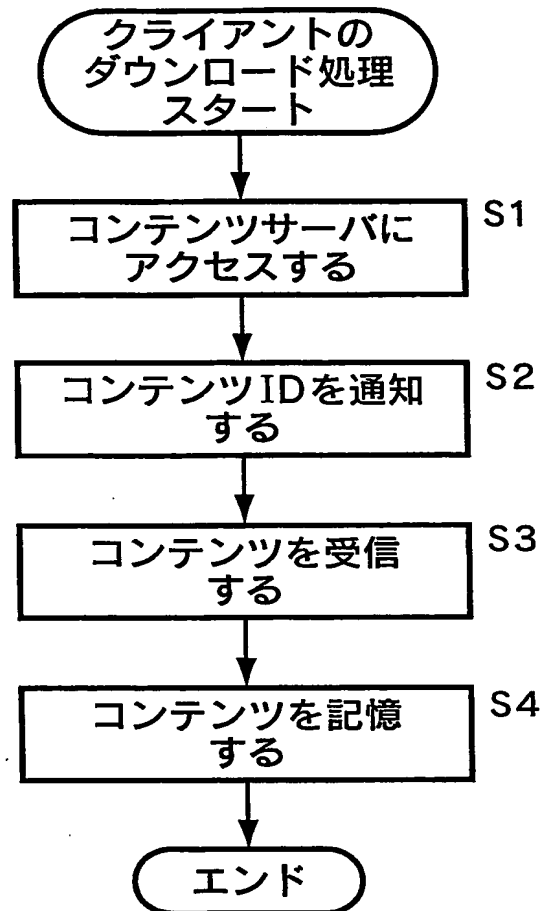


図2



3/14

図 3



4/14

図 4

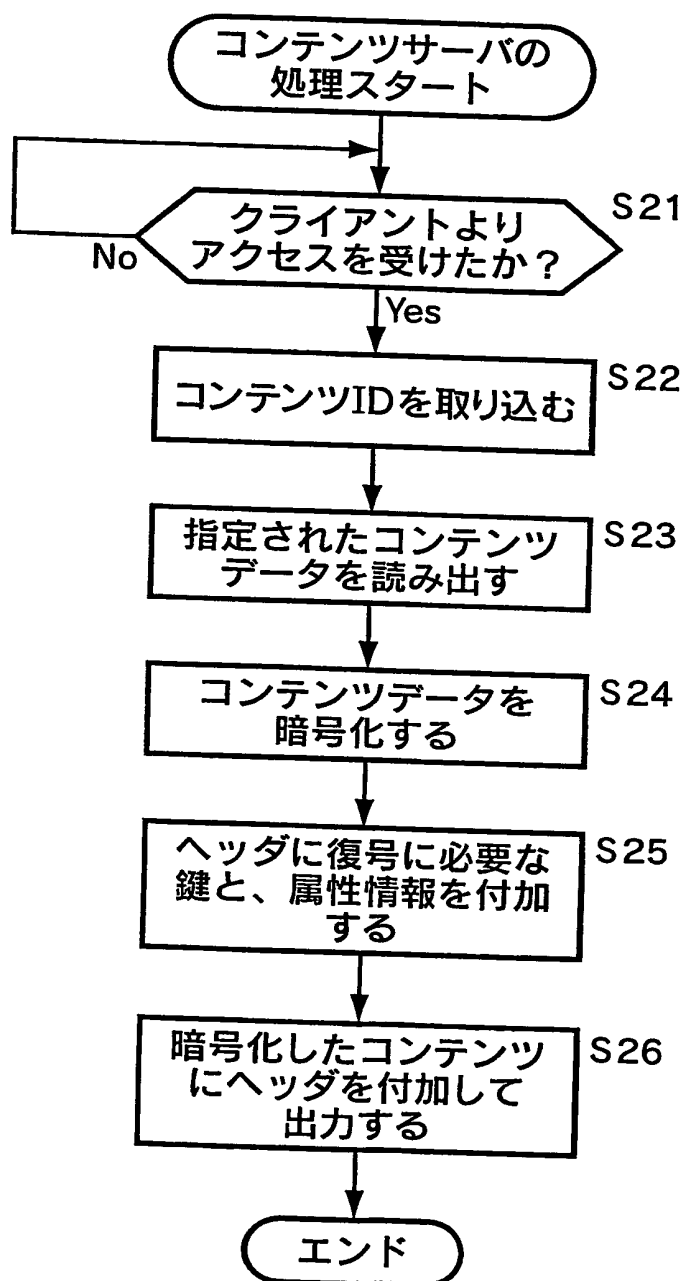
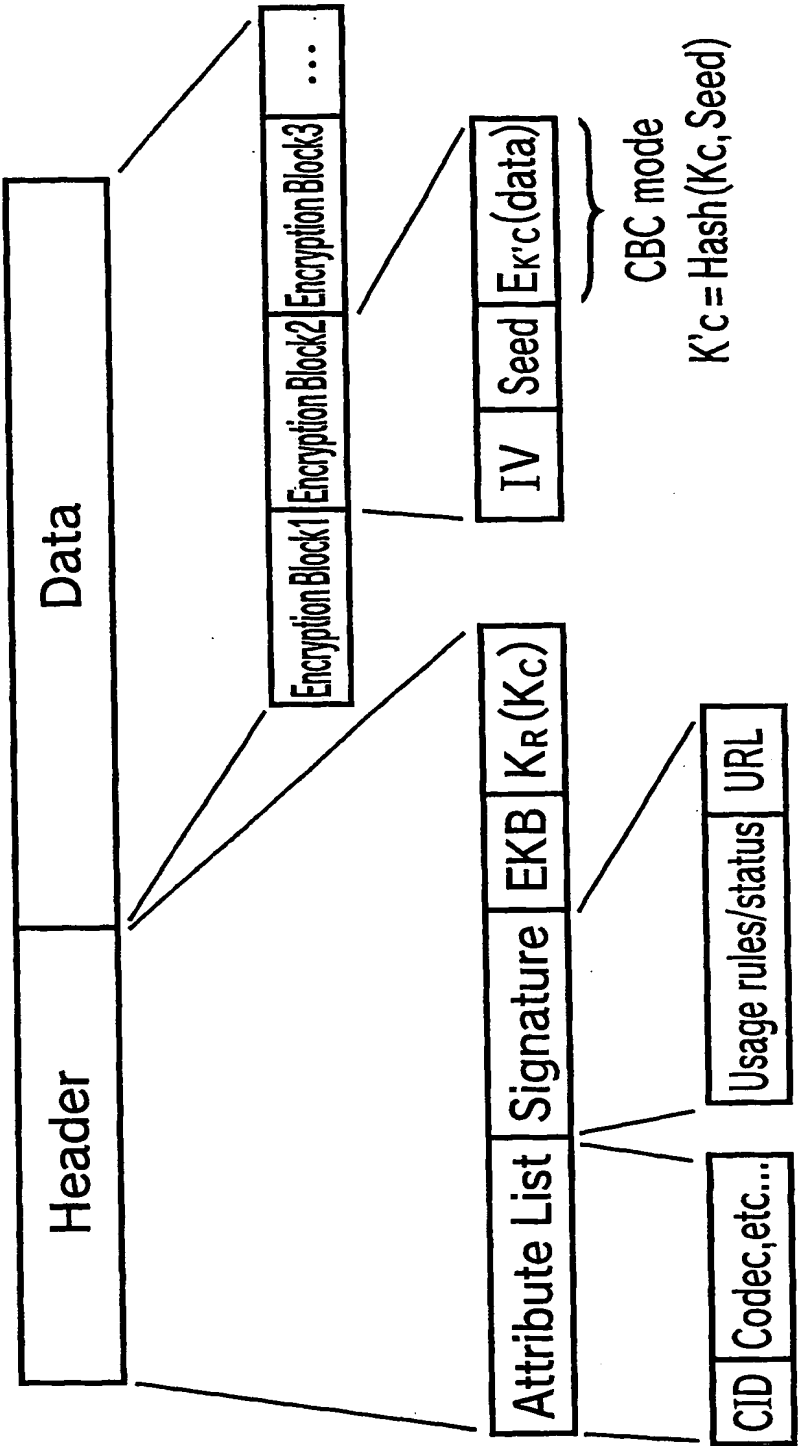


図5



6/14

図 6

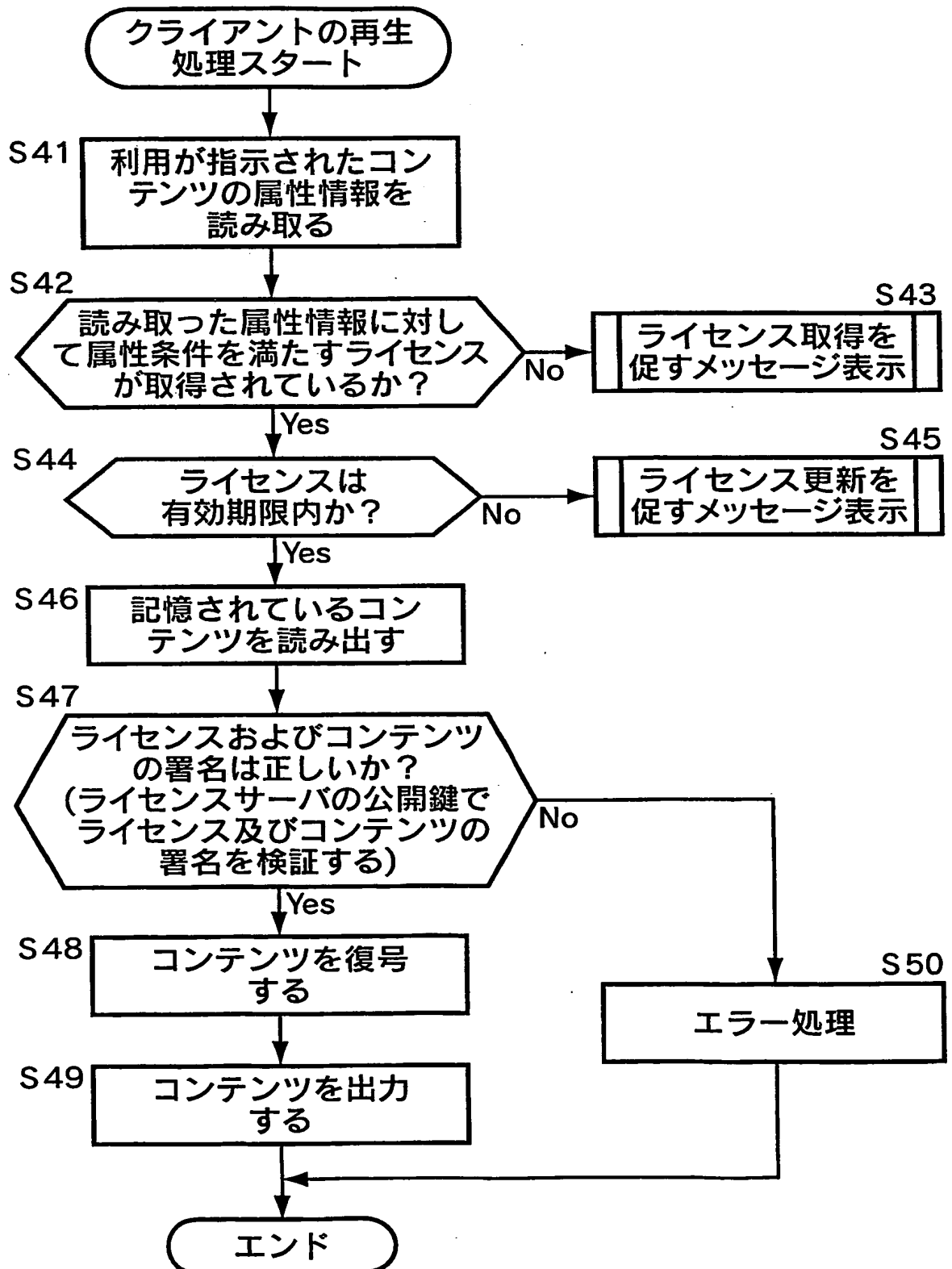
属性項目	説明
CID	コンテンツ ID
RCID	レコード会社 ID
CIID	コンテンツ発行者 ID
AID	アーティスト ID
RelDate	リリース日
GID	ジャンル ID
LID	レーベル ID
SID	サブスクリプション ID
URL	ライセンスサーバの URL

図 7

ライセンス ID
タイムスタンプ
使用期限
属性条件
使用規則
電子署名

7/14

図 8



8/14

図 9

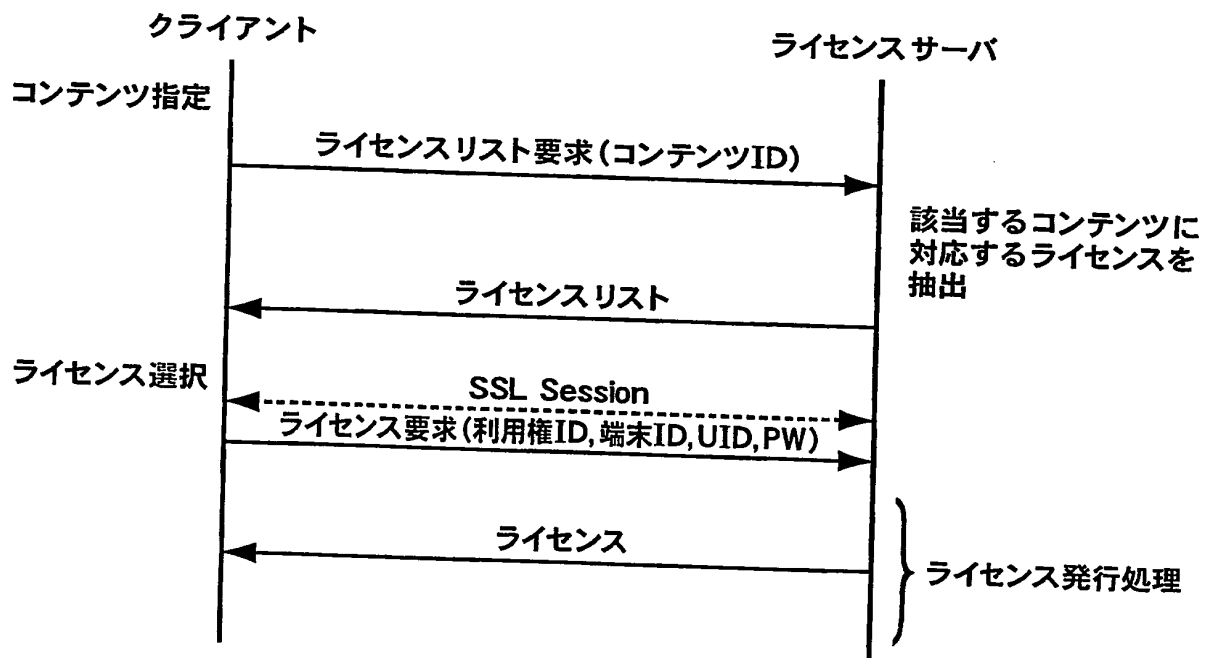
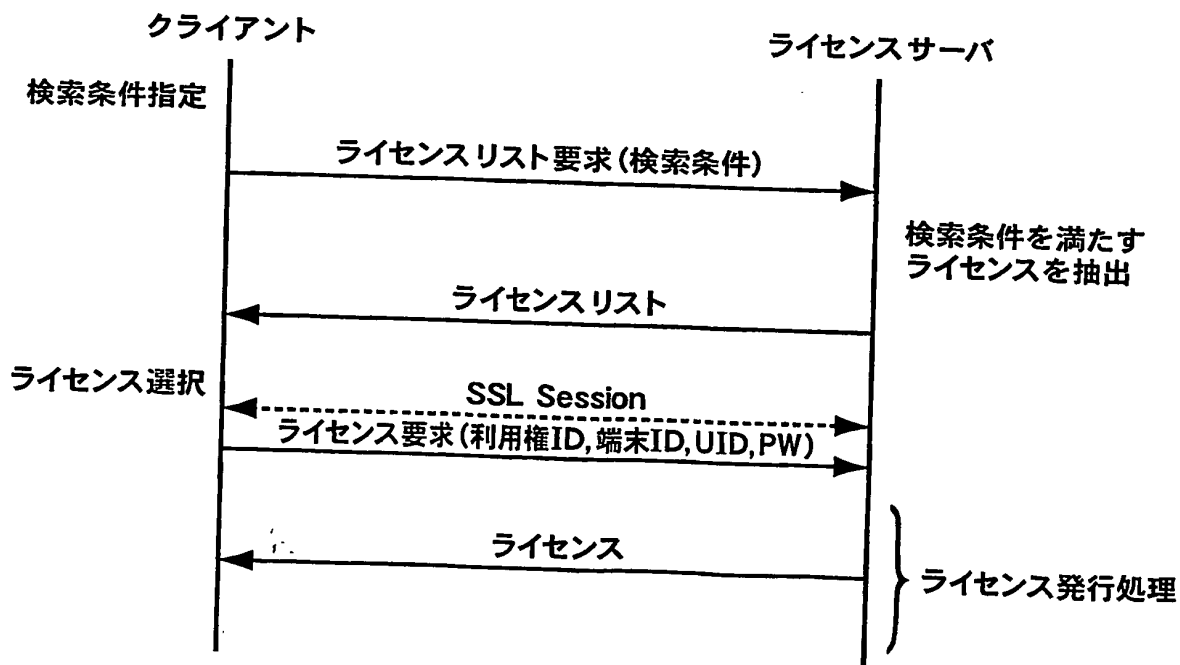
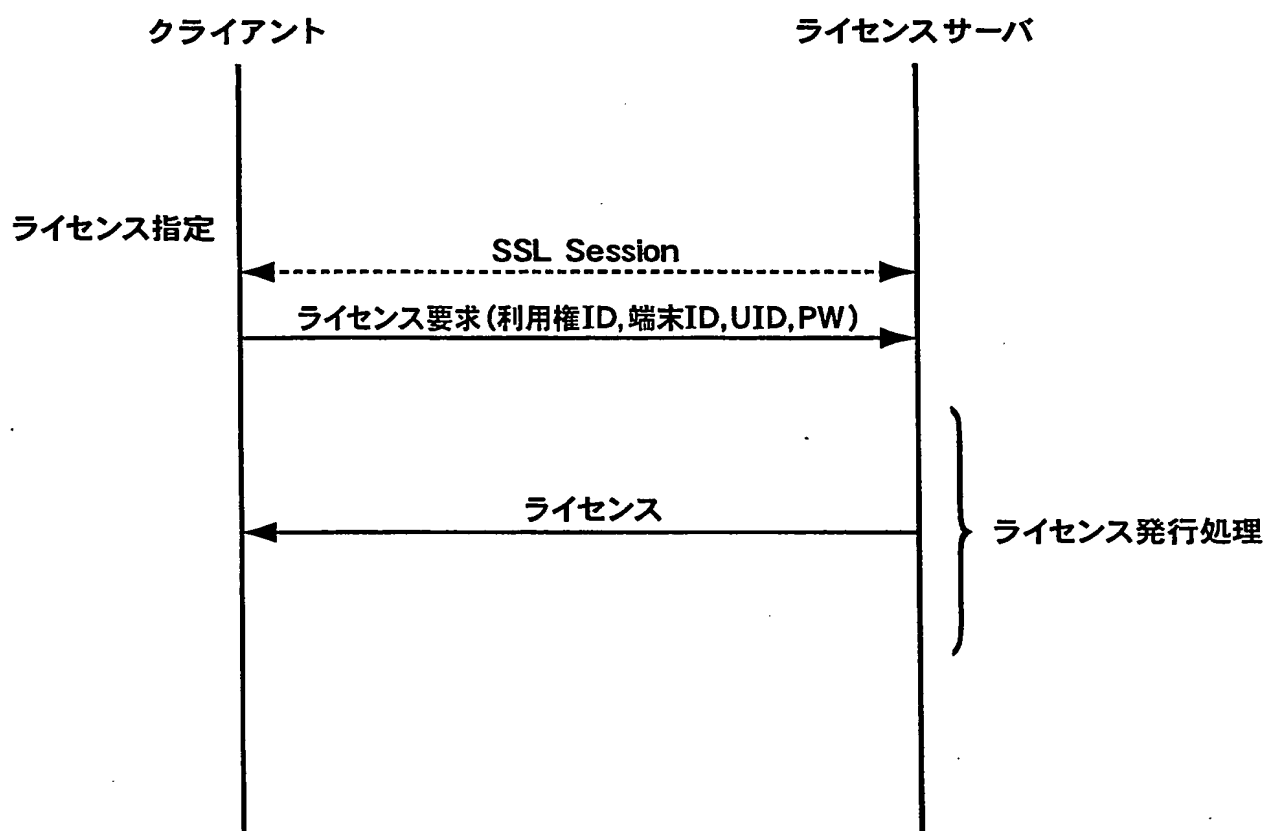


図 10



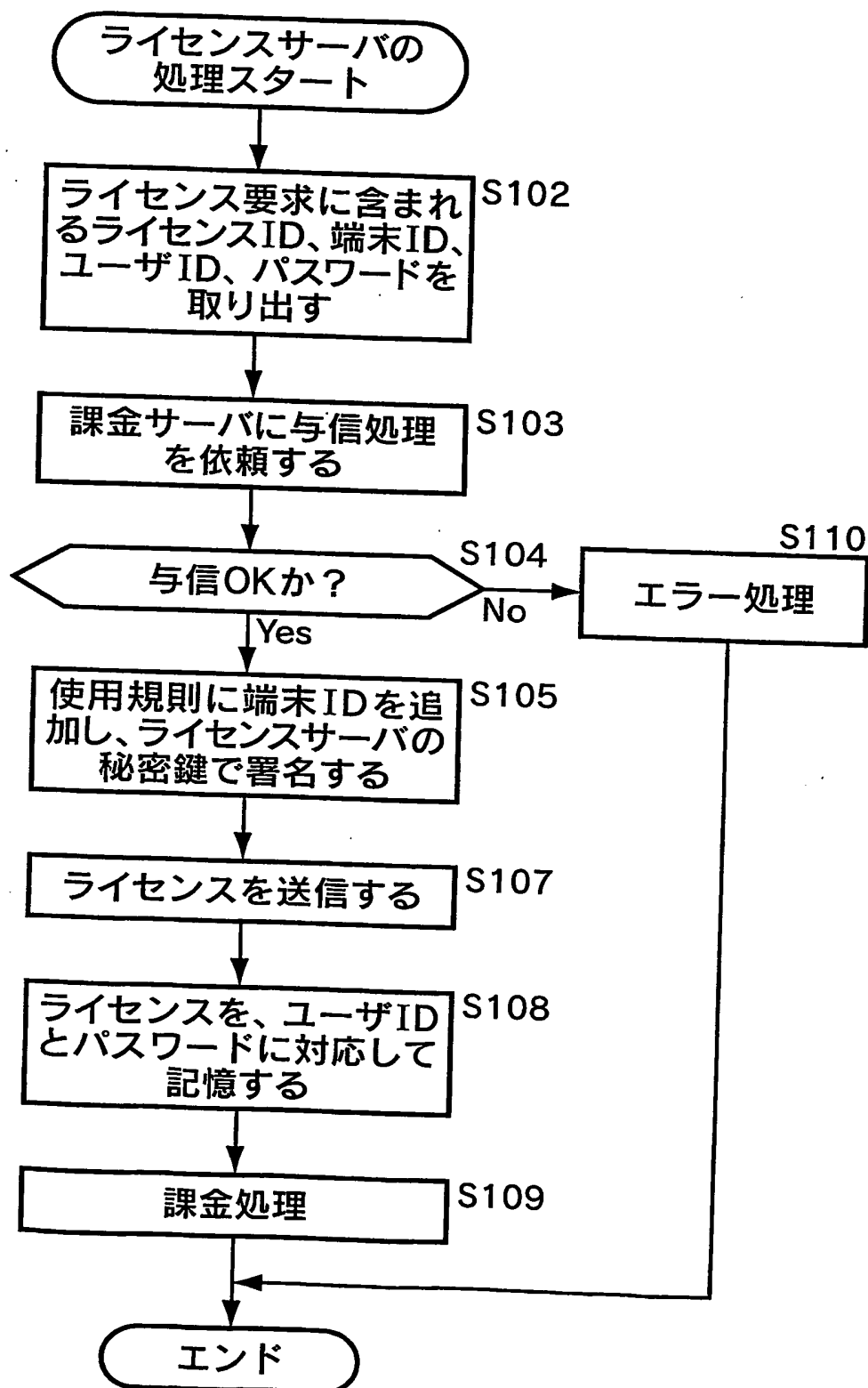
9/14

図 11



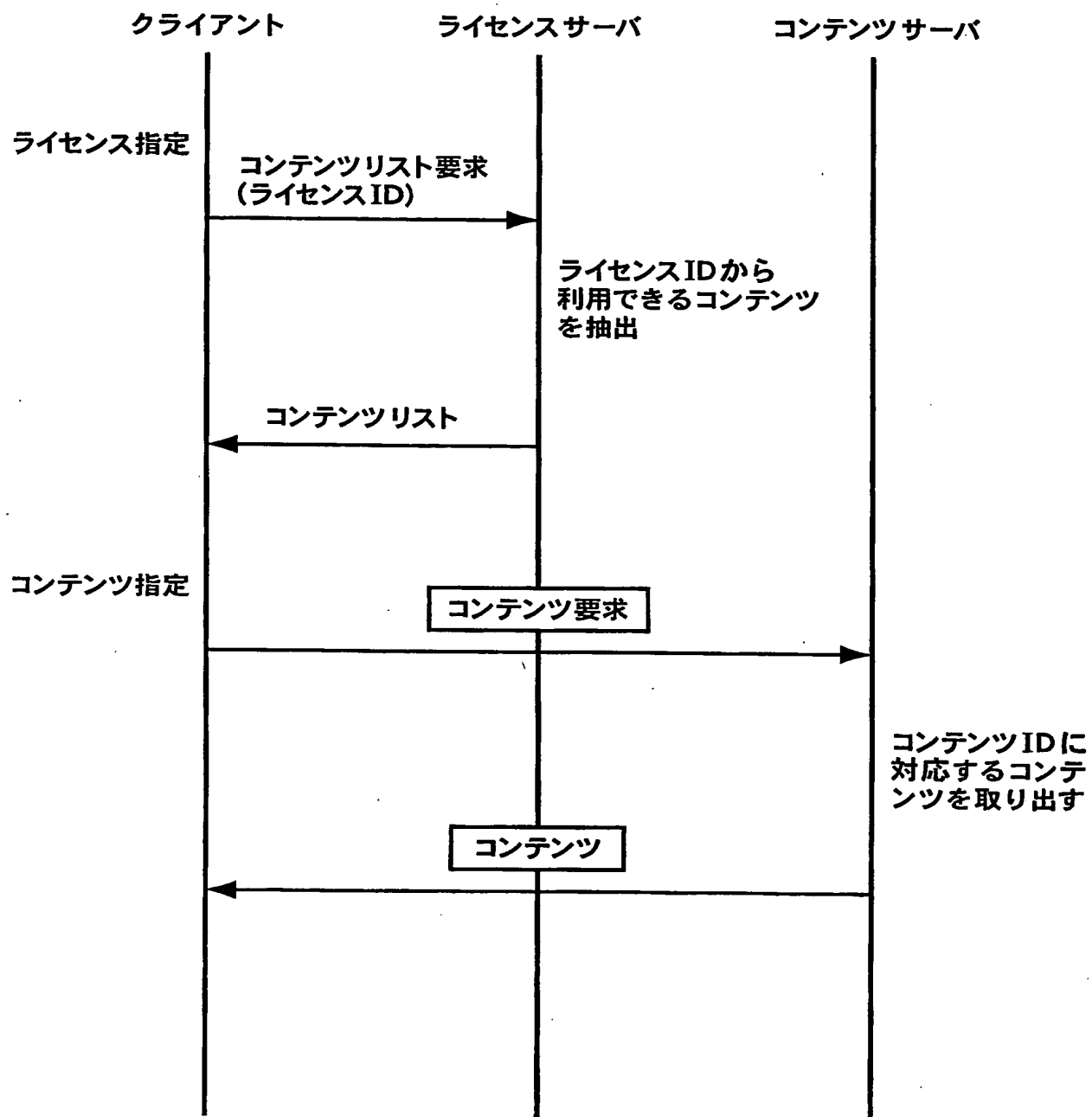
10/14

図12

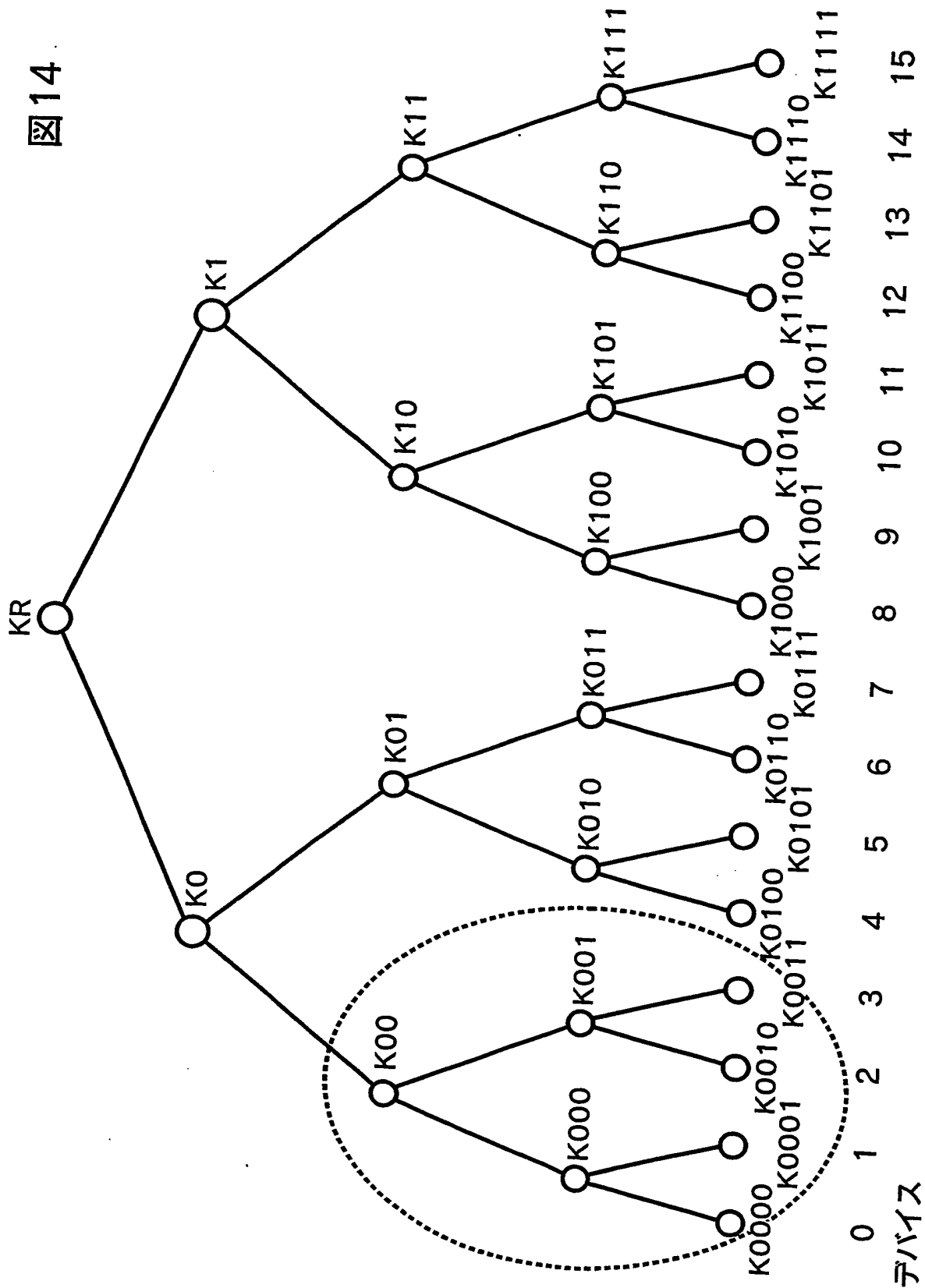


11/14

図 13

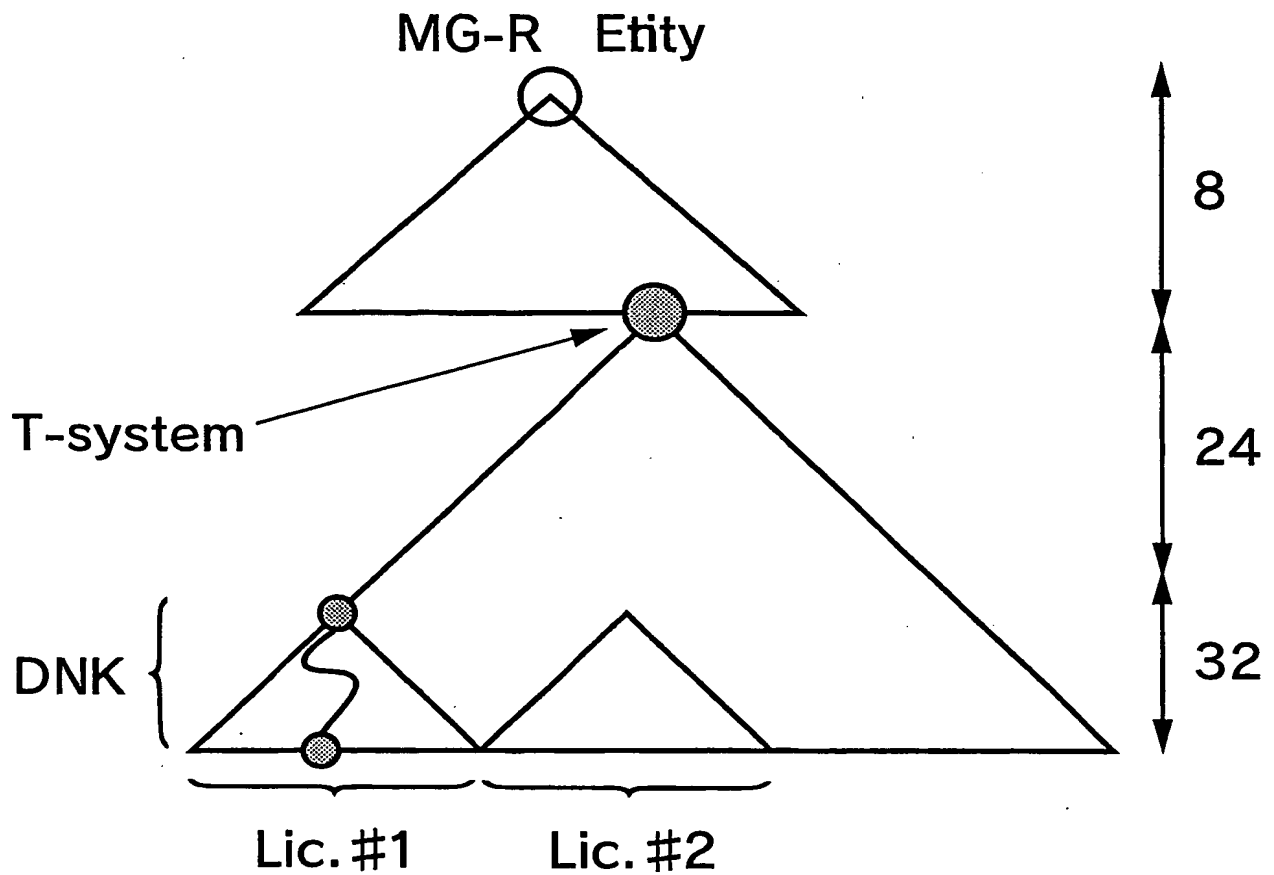


12/14



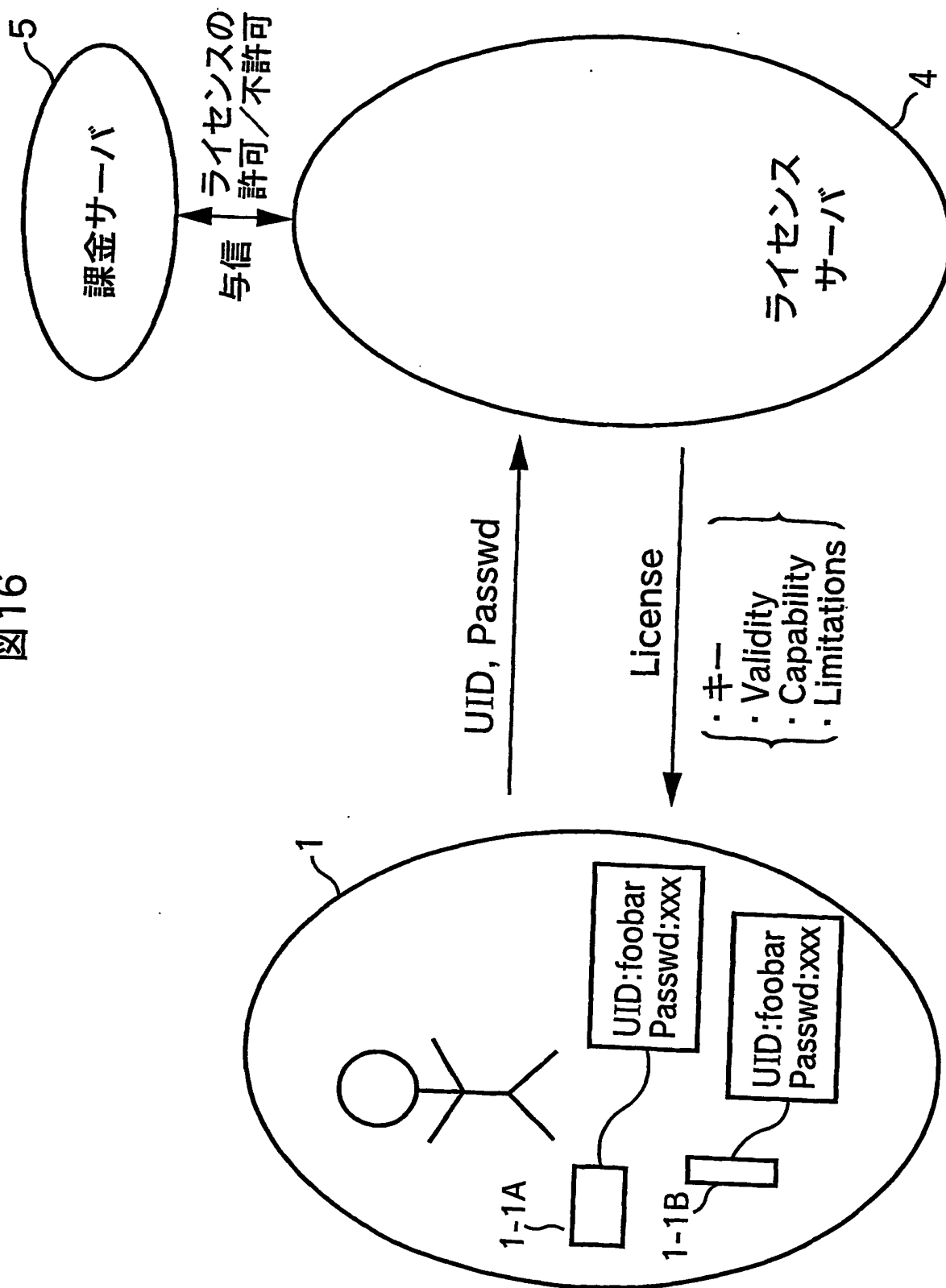
13/14

図 15



14/14

図16



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/12356

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L9/08, G06F17/60, G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L9/08, G06F17/60, G06F15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST FILE(JOIS), WPI, INSPEC(DIALOG), content, attribute, metadata

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 7-74744 A (Waseda University), 17 March, 1995 (17.03.95), Par. Nos. [0022], [0052] to [0053] (Family: none)	1-5, 9-11
Y	JP 2000-293439 A (Fujitsu Ltd.), 20 October, 2000 (20.10.00), Par. Nos. [0069], [0107] to [0108] (Family: none)	1-5, 9-11
Y	"Juraigata Mole o Kakucho shita Online Contents Hanbai System", Information Processing Society of Japan Kenkyu Hokoku, Vol.99, No.11, pages 87 to 93 (99-EIP-3), 30 January, 1999 (30.01.99), 4.3.1 Kenri Hogo Contents Kozo	2

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
07 March, 2003 (07.03.03)Date of mailing of the international search report
18 March, 2003 (18.03.03)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/12356

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 7-105231 A (Nippon Telegraph And Telephone Corp.), 21 April, 1995 (21.04.95), Par. No. [0026] (Family: none)	1-5, 9-11
A	JP 2000-188744 A (Kabushiki kaisha Jisedai Joho Hoso System Kenkyusho), 04 July, 2000 (04.07.00), Par. Nos. [0079] to [0085] (Family: none)	1-5, 9-11
A	EP 1107137 A2 (International Business Machines Corp.), 13 June, 2000 (13.06.00), All pages & JP 2001-274788 A & CN 1306259 A	1-5, 9-11
A	US 2001/0042111 A1 (Matsushita Electric Industrial Co., Ltd.), 15 November, 2001 (15.11.01), All pages & EP 116084 A2 & JP 2001-318848 A & CN 1326145 A	1-5, 9-11

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/12356

Box I Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of claims of the present application are divided into the following three groups:

1. Claims 1-5, 9-11
2. Claims 6, 7
3. Claim 8

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.: 1-5, 9-11

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08, G06F17/60, G06F15/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08, G06F17/60, G06F15/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2003年
 日本国登録実用新案公報 1994-2003年
 日本国実用新案登録公報 1996-2003年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JICSTファイル (JOIS), WPI, INSPEC (DIALOG)
content, attribute, metadata

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 7-74744 A (学校法人早稲田大学) 1995.03.17, 第22, 52-53段落 (ファミリーなし)	1-5, 9-11
Y	JP 2000-293439 A (富士通株式会社) 2000.10.20, 第69, 107-108段落 (ファミリーなし)	1-5, 9-11
Y	従来型電子モールを拡張したオンラインコンテンツ販売システム, 情報処理学会研究報告, Vol.99 No.11, p.87-93 (99-EIP-3) 1999.01.30, 4.3.1権利保護コンテンツ構造	2

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

07.03.03

国際調査報告の発送日

18.03.03

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

中里 裕正



5M

9364

電話番号 03-3581-1101 内線 3597

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 7-105231 A (日本電信電話株式会社) 1995. 04. 21, 第26段落 (ファミリーなし)	1-5, 9-11
A	JP 2000-188744 A (株式会社次世代情報放送システム研究所) 2000. 07. 04, 第79-85段落 (ファミリーなし)	1-5, 9-11
A	EP 1107137 A2 (International Business Machines Corporation) 2000. 06. 13, 全頁を参照 & JP 2001-274788 A & CN 1306259 A	1-5, 9-11
A	US 2001/0042111 A1 (Matsushita Electric Industrial Co., Ltd.) 2001. 11. 15, 全頁を参照 & EP 116084 A2 & JP 2001-318848 A & CN 1326145 A	1-5, 9-11

第I欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項(PCT17条(2)(a))の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 _____ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第II欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

本願の請求の範囲に係る発明は、以下の3群に分けられるものと認める。

1. 請求の範囲 1-5, 9-11
2. 請求の範囲 6, 7
3. 請求の範囲 8

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☒ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

請求の範囲 1-5, 9-11

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLACK (USPTO)